Testimony of James E. Farnan,
Deputy Assistant Director,
Cyber Division,
Federal Bureau of Investigation,
before the
House Committee on Government Reform
May 15, 2003

Thank you for inviting me here today to testify in this hearing at which the Committee is examining privacy and security issues associated with the use of peer-to-peer file sharing programs. This hearing and the Committee's Web page, in which you provide a link to: "Parental Tips for Internet File-Sharing Programs," demonstrate your commitment to improving the abilities of our Nation's families and businesses to be safe, secure, and crime-free while using the Internet as a tool for research, entertainment and commerce. Our work here is vitally important because Internet use grows each day, and each day there are thousands of new victims. My testimony today will address the activities of the FBI's Cyber Division as they relate to a broad spectrum of criminal acts involving identity theft, fraud, information security and computer intrusions.

A May 8th cover story in the Washington Post is nothing new to Americans today. Another gang of thieves was discovered in possession of a "veritable factory for counterfeit credit cards," including "600 pages containing more than 40,000 allegedly stolen names and credit card numbers; more than 100 newly minted cards under 100 different names, featuring the trademark Visa logo." The police also found "stacks of

plastic cards, software to create identity cards, laptop computers, machinery to encode magnetic strips, and a 'skimmer' that captures a facsimile of credit card information and stores it...(and) 16-digit credit card numbers, with their expiration dates, that had been downloaded from one major retail store in the area." As the investigation continues, we will probably find that these criminals have affected the lives of hundreds of victims, perhaps destroying their credit ratings and creating hardships that will take years to abate. These thefts could be the result of computer hacking, insider theft and/or social engineering. The FBI treats each of these techniques as criminal acts, and we continue to seek out those who would use them to illegally enrich themselves. Stolen information can also be sold and used to establish new identities for fugitives or terrorists. In these cases, identity theft can have much more serious consequences.

The Federal Trade Commission's annual report lists identity theft as it's most substantial category of reported crime, at 43% of the total. Its impact on citizens and businesses both domestically and abroad, as well as the growing number of ways that such schemes can be initiated or advanced, primarily through the Internet, is a priority interest for the FBI. An understanding of the scope of the problem can only be gained by identifying the variety of acts related to identity theft, including insider theft, hacking, spam, spoofing, account hijacking, auction fraud and peer to peer (P2P) sharing. Below are some examples and definitions:

Identity Theft

Identity theft is the fraudulent use of an individual's personal identifying information, such as a social security number, mother's maiden name, date of birth or bank account number. Identity theft includes alias identity crimes in which an individual's true identity is completely fabricated and not identified with a real person, whether living or deceased. Identity theft is normally a preliminary step toward committing other crimes. Some will engage in identity theft for financial gain, others to avoid arrest or detection, attain legal immigrations status, or obtain government benefits. Victims of identity theft may not realize that someone has stolen their identity until they are denied credit or until a creditor attempts to collect an unpaid bill. Identity theft can be a component of many crimes, including bank fraud, telemarketing fraud, Ponzi schemes, credit card fraud, bankruptcy fraud, money laundering, insurance fraud, cyber crimes and unlawful flight to avoid prosecution (fugitives). The FBI's Criminal Investigative Division has recently begun to track identity theft as a component of other criminal activities. Their efforts will statistically measure the increase in crimes involving identity theft.

Spam

Spam generally refers to unsolicited incoming messages inviting an individual to buy, sell, invest or join a certain club. Significantly, The Internet Fraud Complaint Center (IFCC) is seeing more and more spam referrals in which individuals are being directed to provide certain personal, including financial and password information, to

remedy a credit problem, update their account information, or to avoid being part of an undesirable mailing list.

Spoofing

In one investigation, subjects collected individual e-mail addresses from Internet chat rooms and other Internet sources. The subjects then sent e-mail to individuals requesting credit card and personal information. The e-mail appeared to be from the victims' Internet service provider (ISP) (spoofed e-mail) claiming that the victims needed to provide current billing information. Victims would respond and provide their credit card and personal information, believing the information was going to their ISP. The subjects used credit card and personal information to obtain cash advances and purchase items utilizing the Internet.

In another investigation, subjects established a spoofed web-site, which was made to appear to be a U.S financial institution. This site was used to lure victims into providing personal financial information, including credit card and debit card numbers, which were than transmitted abroad to criminals who used the stolen cards at automatic teller machines throughout Europe.

Auction Fraud and Account Hijacking

Over the past year, the IFCC has received many complaints regarding auction

sites wherein a customer's account was hijacked. In such cases the perpetrator gains unauthorized access (via computer intrusion) to customer accounts, determines which accounts have a good reference/feedback history, and represent themselves as that individual, selling merchandise, which is ultimately never delivered. Losses in such schemes range from hundreds of dollars to upwards of $100K with numerous victims. These types of schemes can also result in identity theft when unsuspecting customers provide credit card information to the criminal.

Computer Intrusion/Hacking

Computer intrusions are a different category from most fraud schemes. Many intrusions are never reported because companies fear a loss of business from reduced consumer confidence in their security measures or from a fear of lawsuits. Most of the outsider-intrusions cases opened today are the result of a failure to patch a known vulnerability for which a patch has been issued. Theft of consumer information from a computer system can only be facilitated two ways: by insiders or by outside hackers. Insiders have various motivations, including retribution and money. Outsiders are usually motivated by challenge and/or greed.

The IFCC recently received a referral through its website, in which the computer system of a small business that sold certain pharmaceutical products online was

compromised by a hacker, who acquired credit card numbers, and the names and addresses of approximately 200 customers. This information was then posted on an Internet message board, where access to this personal data could be gained by anyone with an computer and an Internet account.

The FBI has seen a steady increase in computer intrusion/hacking cases. With the proliferation of "turn key" ("turn key" in that no special knowledge is needed to apply the tool - you only need to download the tool and apply it) hacking tools/utilities available on the Internet, this trend is not surprising. In many cases, computer intrusion incidents may represent the front end of a criminal matter, where credit card fraud, economic espionage, and/or identity theft represent the final result, and the intended purpose of the scheme. In some cases, a computer intrusion may also have been for the purpose of installing a Trojan, or back door that the hacker can later access. The hacker may want to launch a denial of service (DOS) attack, or to access personal financial, or other sensitive data contained on that system.

P2P Sharing

P2P networks primarily serve as a "come and get it" resource on the Internet. In using such a utility, the user specifically searches for the item they want, e.g. music, images, or software. The most significant criminal activity involving P2P sharing centers largely on intellectual property rights (music and software piracy) matters, an area in which the FBI has been working closely with private industry. The FBI has also seen an

increase in P2P sharing of child pornography files.

Although no instances of identity theft have been reported to be associated with P2P networks, there are several dynamics that should also be considered:

The FBI has seen an increasing number of instances where a victim has determined that a Trojan/back door was installed on their computer during a download from a P2P network. In some cases, the victim also learned that personal, financial information had also been removed from their computer via the back door.

In addition to traditional Trojans/back doors, The FBI has seen an increase in matters where certain "bots" (active Trojans) have been installed inadvertently via a P2P download. In these instances, the victim computer, via the bot, essentially reports to a designated Internet relay chat (IRC) site, awaiting further instructions from its creator. The creator of the bot will often use the compromised computers to launch coordinated denial of service attacks against a targeted site or sites. These bots could also be used to retrieve sensitive information from victim computers in furtherance of an identity theft scheme.

A person using P2P utilities for unauthorized or illegal purposes is not as likely to tell the FBI that an exploit (back door) was found on their system, or that as a result, certain personal or financial information may have been taken. The FBI has been made aware of instances where Trojans or bots have been found on computer systems where

P2P programs are present, and where certain personal, financial or other sensitive information has been taken.

The FBI is in a unique position to respond to most cyber crimes, because it is the only Federal agency that has the statutory authority, expertise, and ability to combine the counterterrorism, counterintelligence, and criminal resources needed to effectively neutralize, mitigate, and disrupt illegal computer-supported operations.

The FBI's Cyber Division

The FBI's reorganization of the last two years included the goal of making our cyber investigative resources more effective. In July 2002, the reorganization resulted in the creation of the FBI's Cyber Division. In prioritizing Cyber Crime, the FBI recognizes that all types of on-line crime are on the rise.

The Cyber Division addresses cyber threats in a coordinated manner, allowing the FBI to stay technologically one step ahead of the cyber adversaries threatening the United States. The Cyber Division addresses all violations with a cyber nexus, which often have international facets and national economic implications. The Cyber Division also simultaneously supports FBI priorities across program lines, assisting counterterrorism, counterintelligence, and other criminal investigations when aggressive technological investigative assistance is required. The Cyber Division will ensure that agents with specialized technology skills are focused on cyber related matters.

At the Cyber Division we are taking a two-tracked approach to the problem. One avenue is identified as traditional criminal activity that has migrated to the Internet, such as Internet fraud, on-line identity theft, Internet child pornography, theft of trade secrets, and other similar crimes. The other, non-traditional approach consists of Internet-facilitated activity that did not exist prior to the establishment of computers, networks, and the World Wide Web. This encompasses “cyber terrorism,” terrorist threats, foreign intelligence operations, and criminal activity precipitated by illegal computer intrusions into U.S. computer networks, including the disruption of computer supported operations and the theft of sensitive data via the Internet. The FBI assesses the cyber-threat to the U.S. to be rapidly expanding, as the number of actors with the ability to utilize computers for illegal, harmful, and possibly devastating purposes is on the rise.

The mission of the Cyber Division is to: (1) coordinate, supervise and facilitate the FBI's investigation of those federal violations in which the Internet, computer systems, or networks are exploited as the principal instruments or targets of terrorist organizations, foreign government sponsored intelligence operations, or criminal activity and for which the use of such systems is essential to that activity; (2) form and maintain public/private alliances in conjunction with enhanced education and training to maximize counterterrorism, counterintelligence, and law enforcement cyber response capabilities, and (3) place the FBI at the forefront of cyber investigations through awareness and exploitation of emerging technology.

To support this mission we are dramatically increasing our cyber training program and international investigative efforts. Consequently, specialized units are now being created at FBI Headquarters to provide training not only to the 60 FBI cyber squads, but also to the other agencies participating in existing or new cyber-related task forces in which the FBI is a participant. This training will largely be provided to investigators in the field. A number of courses will be provided at the FBI Academy at Quantico.

The importance of partnerships like law enforcement cyber task forces and alliances with industry can not be overstated. Those partnerships help develop early awareness of, and a coordinated, proactive response to, the crime problem. The cyber crime problem is constantly changing, requiring law enforcement to develop a flexible and dynamically evolving approach as well. Critical infrastructures and e-commerce are truly on the "front lines" and most often better positioned to identify new trends in cyber crime. Similarly, because of the actual and potential economic impact of cyber criminals, private industry has a vested interest in working with law enforcement to effectively detect, deter and investigate such activity.

The Cyber Division is also embarking on a significant effort to improve our overseas investigative capabilities. We will be training more foreign police officers, and sending FBI personnel throughout the world to help investigate cyber crimes when invited or allowed by a host country. We believe this dramatic increase in high tech training and overseas investigations is justified by the increasing internationalization of

on-line crime and terrorist threats.

Through the Internet Fraud Complaint Center (IFCC), established in 1999 in partnership with the National White Collar Crime Center (NW3C), the FBI has appropriately positioned itself at the gateway of incoming intelligence regarding cyber crime matters. The IFCC receives complaints regarding a vast array of cyber crime matters, including: computer intrusions, identity theft, economic espionage, credit card fraud, child pornography, on-line extortion and a growing list of internationally spawned Internet fraud matters. The IFCC received 75,000 complaints in 2002, and is now receiving more than 9000 complaints per month. We expect that number to increase significantly as the American and international communities become more aware of our mission and capabilities. Later this year, the IFCC will be renamed as the Internet Crime Complaint Center (IC3) to more accurately reflect its mission.

If the IFCC received an intrusion report from a company in Birmingham, Alabama, we would first attempt to locate where the intrusion took place. That same company may have its servers in Minneapolis, while the intruder is routing attacks through Internet providers in California and Europe. If the servers in Minneapolis were hacked, the Minneapolis Cyber Crime Task Force would be assigned the lead on the case. The leads could start in California, but end up in Eastern Europe, Nigeria or even back to Birmingham, if an insider was involved. One of the FBI's Computer Analysis Response Teams (CART) would be called upon to preserve computer forensic evidence, and that evidence could be forwarded to one of our new Regional Crime

Forensic Labs, now located in Chicago, Dallas and San Diego. The Lab would determine the extent and duration of the intrusion, and whether the attacker came from inside or outside the company. Depending on the sophistication of the intruder, the case can be cracked in a few days or take years. It is important to note again that an intrusion may only be the first indication of another crime. An intrusion could finally result in anything from identity theft, terrorism, or espionage. Cases are routinely complex, and often involve international connections. The following cases serve as examples of typical cyber crimes:

Raymond Torricelli, aka "rolex"

Raymond Torricelli, aka "rolex," the head of a hacker group known as "#conflict," was convicted for, among other things, breaking into two computers owned and maintained by the National Aeronautics and Space Administration's Jet Propulsion Laboratory ("JPL"), located in Pasadena, California, and using one of those computers to host an Internet chat-room devoted to hacking.

Torricelli admitted that, in 1998, he was a computer hacker, and a member of a hacking organization known as "#conflict." Torricelli admitted that he used his personal computer to run programs designed to search the Internet, and seek out computers which were vulnerable to intrusion. Once such computers were located, Torricelli's computer

obtained unauthorized access to the computers by uploading a program known as "rootkit." The file, "rootkit," is a program which, when run on computer, allows a hacker to gain complete access to all of a computer's functions without having been granted these privileges by the authorized users of that computer.

One of the computers Torricelli accessed was used by NASA to perform satellite design and mission analysis concerning future space missions, another was used by JPL's Communications Ground Systems Section as an e-mail and internal web server. After gaining this unauthorized access to computers and loading "rootkit," Torricelli, under his alias "rolex," used many of the computers to host chat-room discussions.

Torricelli admitted that, in these discussions, he invited other chat participants to visit a website which enabled them to view pornographic images and that he earned 18 cents for each visit a person made to that website. Torricelli earned approximately $300-400 from per week from this activity. Torricelli also pled guilty to intercepting user names and passwords traversing the computer networks of a computer owned by San Jose State University. In addition, Torricelli pled guilty to possession of stolen passwords and user names which he used to gain free Internet access, or to gain unauthorized access to still more computers. Torricelli

admitted that when he obtained passwords which were encrypted, he would use a password cracking program known as"John-the-Ripper" to decrypt the passwords. He also pled guilty to possessing stolen credit card numbers that he obtained from other individuals and stored on his computer. Torricelli admitted that he used one such credit card number to purchase long distance telephone service.

Much of the evidence obtained against Torricelli was obtained through a search of his personal computer. In addition to thousands of stolen passwords and numerous credit card numbers, investigators found transcripts of chat-room discussions in which Torricelli and members of "#conflict" discussed, among other things, (1) breaking into other computers; (2) obtaining credit card numbers belonging to other persons and using those numbers to make unauthorized purchases; and (3) using their computers to electronically alter the results of the annual MTV Movie Awards. This case illustrates the wide variety of criminal acts which can result from security vulnerabilities.

Raphael Gray, aka "Curador"

On March 1, 2000, a computer hacker using the name "Curador" compromised several e-commerce websites in the U.S., Canada, Thailand, Japan and the United Kingdom, and stole as many as 28,000

credit card numbers with losses estimated to be at least $3.5 million. Thousands of credit card numbers and expiration dates were posted to various Internet websites.. After an extensive investigation, on March 23, 2000, the FBI assisted the Dyfed Powys (Wales, UK) Police Service in a search at the residence of "Curador," Raphael Gray. Mr. Gray, age 18, was arrested and charged in the UK along with a co-conspirator under the UK's Computer Misuse Act of 1990. This case illustrates the benefits of law enforcement and private industry around the world working together in partnership on computer crime investigations.

Cyber crime continues to grow at an alarming rate, and identity theft is a major part of the increase. Criminals are only beginning to explore the potential of crime via peer-to-peer networks while they continue to steal information by hacking, insider exploitation and social engineering. The FBI is grateful for the efforts of your Committee and others dedicated to the safety and security of our Nation's families and businesses. The FBI will continue to work with your Committee and aggressively pursue cyber criminals as we strive to stay one step ahead of them in the cyber crime technology race.

I thank you for your invitation to speak to you today and on behalf of the FBI look forward to working with you on this very important topic.